Flexible NetFlow の設定

Flexible NetFlow の前提条件

- 次のコマンドで定義される Flexible NetFlow の key フィールドについてよく理解していること。
  - **match flow**
  - **match interface**
  - **match** {**ipv4** | **ipv6**}
  - **match routing**
  - **match transport**
- 次のコマンドで定義される Flexible NetFlow の nonkey フィールドについてよく理解していること。
  - **collect counter**
  - **collect flow**
  - **collect interface**
  - **collect**{**ipv4** | **ipv6**}
  - **collect routing**
  - **collect timestamp sys-uptime**

- **collect transport**

- ネットワーキング デバイスで、Flexible NetFlow がサポートされた Cisco リリースが稼働していること。

IPv4 トラフィック

- ネットワーキング デバイスが IPv4 ルーティング用に設定されていること。
- Cisco Express Forwarding またはdistributed Cisco Express Forwarding のいずれかが、デバイスおよびFlexible NetFlow を有効化するすべてのインターフェイスで有効化されていること。

IPv6 トラフィック

- ネットワーキング デバイスが、IPv6 ルーティング用に設定されていること。
- Cisco Express Forwarding IPv6 または分散型 Cisco Express Forwarding のいずれかが、デバイスおよび Flexible NetFlow を有効化するすべてのインターフェイスで有効化されていること。

Flexible Netflow に関する制約事項

次に、Flexible NetFlow に関する制約事項を示します。

- Flexible NetFlow は、レイヤ 2 ポートチャネル インターフェイスではサポートされませんが、レイヤ 2 ポートチャネル メンバ ポートではサポートされます。
- Traditional NetFlow のアカウンティングはサポートされていません。
- Flexible NetFlow バージョン 9 およびバージョン 10 のエクスポートフォーマットがサポートされています。ただし、エクスポートプロトコルが設定されていない場合は、バージョン 9 のエクスポートフォーマットがデフォルトで適用されます。
- 有線 Application Visibility and Control（AVC）トラフィックの場合、システム上の 1 つ以上のレイヤ 2 またはレイヤ 3 の物理インターフェイスに設定できるフローモニタは 1 つのみです。
- Flexible NetFlow および NBAR は同じインターフェイスで同時に設定できません。
- レイヤ 2、IPv4、および IPv6 のトラフィック タイプがサポートされています。異なるトラフィック タイプの複数のフロー モニタを、指定したインターフェイスと方向に適用できます。同じトラフィック タイプの複数のフロー モニタを指定したインターフェイスと方向には適用できません。
- レイヤ 2、VLAN、レイヤ 3 および SVI インターフェイスがサポートされています。ただし、デバイスはトンネルをサポートしていません。
- 次のサイズの NetFlow テーブルがサポートされています。

トリム レベル	入力 NetFlow テーブル	出力 NetFlow テーブル
Network Essentials	32 K	32 K
Network Advantage	32 K	32 K

- スイッチのタイプに応じて、スイッチには 1 個または 2 個の転送 ASIC があります。上の表に示されている容量は、コア単位または ASIC 単位です。
- スイッチは最大 4 つの ASIC をサポートします。各 ASIC には 2 つのコアがあります。各 TCAM は最大 1024 の入力エントリと 2048 の出力エントリを処理できますが、各コアには 32K の入力と 32K の出力エントリがあります。
- NetFlow テーブルは個別のコンパートメントにあり、組み合わせることはできません。パケットを処理したコアに応じて、対応したコアのテーブルにフローが作成されます。
- NetFlow ハードウェアの実装では、4 台のハードウェア サンプラーがサポートされています。1/2 ～ 1/1024 のサンプラー レートを選択できます。ランダム サンプリングと確定的サンプリングの両方のモードがサポートされています。
- NetFlow ハードウェアの内部では、ハッシュ テーブルが使用されています。ハードウェア内でハッシュ衝突が発生する場合があります。したがって、内部の連想メモリ（CAM）でオーバーフローが発生しても、実際の NetFlow テーブルの使用率は約 80 % しかない場合があります。
- フローに使用されるフィールドによって異なりますが、単一のフローは 2 個の連続したエントリを取得できます。IPv6 フローとデータリンク フローも 2 個のエントリを取得します。この場合、NetFlow エントリを効果的に使用すれば、テーブル サイズの半分で済みます。これは、上記のハッシュ衝突の制限とは別です。
- デバイスは、最大 15 個のフローモニタをサポートしています。
- NetFlow ソフトウェアの実装では、分散 NetFlow エクスポートがサポートされるため、フローが作成された同じデバイスからフローがエクスポートされています。
- 入力フローは最初にフローのパケットを受信した ASIC にあります。出力フローは、パケットが実際にデバイスセットアップを残した ASIC にあります。
- バイト カウント フィールドのレポート値（「bytes long」と呼ばれる）は、レイヤ 2 パケット サイズの 18 バイトです。従来のイーサネット トラフィック（802.3）の場合、これは正確です。他のすべてのイーサネット タイプの場合、このフィールドは正確ではありません。「bytes layer2」フィールドを使用すると、常に正確なレイヤ 2 パケット サイズが報告されます。サポートされる Flexible NetFlow フィールドについては、トピック「Supported Flexible NetFlow Fields」を参照してください。
- Flexible NetFlow エクスポートは、イーサネット管理ポート（GigabitEthernet 0/0）ではサポートされていません。
- フロー レコードに送信元グループ タグ（SGT）と宛先グループ タグ（DGT）のフィールド（またはこの 2 つのいずれかのフィールド）だけが含まれる場合、両方の値を適用できないとしても、SGT と DGT に値ゼロを設定したフローが作成されます。フロー レコード

には、SGT および DGT フィールドと一緒に、送信元および宛先 IP アドレスが含まれる必要があります。

- Cisco TrustSec 以外のインターフェイスでは、SGT 値がゼロの場合、コマンドヘッダーがないことを意味します。Cisco TrustSec インターフェイスでは、SGT 値がゼロの場合、不明タグであることを意味します。
- Quality of Service（QoS）のマークが付けられたパケットが入力方向に NetFlow が設定されているインターフェイスで受信されると、パケットの QoS 値が NetFlow コレクタによってキャプチャされます。ただし、パケットが出力方向に NetFlow が設定されているインターフェイスで受信されると、パケットの QoS 値はコレクタによってキャプチャされます。
- IPv6 フローモニタの場合、送信元グループタグ（SGT）フィールドと宛先グループタグ（DGT）フィールドは、MAC アドレスフィールドと共存できません。
- NetFlow レコードは、マルチプロトコル ラベル スイッチング対応（MPLS 対応）インターフェイスをサポートしません。
- MPLS ネットワーク内の MPLS ラベルに基づくデータキャプチャはサポートされていません。MPLS タグ付きパケットの IP ヘッダーフィールドのキャプチャはサポートされていません。
- 出力フローモニタは、EoMPLS モードまたは L3VPN Per-Prefix モードで出力されるフローをキャプチャしません。
- フローエクスポータは、テンプレートデータのタイムアウト期間が終了した後にのみ、フローデータをエクスポートします。VPN ID の変更や VRF の削除などの設定変更は、タイムアウト期間の終了後に有効になります。
- フローモニタは、レイヤ 3 物理インターフェイスと論理インターフェイス（レイヤ 3 ポートチャネル インターフェイス、レイヤ 3 ポートチャネルメンバ、スイッチ仮想インターフェイス（SVI）など）間で共有することはできませんが、論理インターフェイス間またはレイヤ 3 物理インターフェイス間で共有できます。

Flexible NetFlow に関する情報

ここでは、Flexible Netflow について説明します。

Flexible NetFlow の概要

Flexible NetFlow ではフローを使用して、アカウンティング、ネットワークモニタリング、およびネットワークプランニングに関連する統計情報を提供します。

フローは送信元インターフェイスに届く単方向のパケット ストリームで、キーの値は同じです。キーは、パケット内のフィールドを識別する値です。フローを作成するには、フロー レコードを使用して、フロー固有のキーを定義します。

デバイスは、ネットワークの変則性とセキュリティの高度な検出を可能にする Flexible NetFlow 機能をサポートします。フレクシブル NetFlow 機能を使用すると、大量の定義済みフィールドの集合からキーを選択することで、そのアプリケーションに最適なフロー レコードを定義できます。

1 つのフローと見なされるパケットでは、すべてのキー値が一致している必要があります。フローは、設定したエクスポート レコード バージョンに基づいて、関係のある他のフィールドを集めることもあります。フローは Flexible NetFlow キャッシュに格納されます。

エクスポータを使用して Flexible NetFlow がフローのために収集するデータをエクスポートし、Flexible NetFlow コレクタなどのリモートシステムにこのデータをエクスポートできます。Flexible NetFlow コレクタは、IPv4 または IPv6 アドレスを使用できます。

モニタを使用してフローのために収集するデータのサイズを定義します。モニタで、フローレコードおよびエクスポータを Flexible NetFlow キャッシュ情報と結合します。

Cisco IOS XE 16.12.1 リリース以降、Flexible NetFlow 上の送信元グループタグ（SGT）および宛先グループタグ（DGT）フィールドは、IPv6 トラフィックでサポートされます。

以前の NetFlow と Flexible NetFlow の利点

Flexible NetFlow ではフローをユーザが定義できます。次に、Flexible NetFlow の利点を示します。

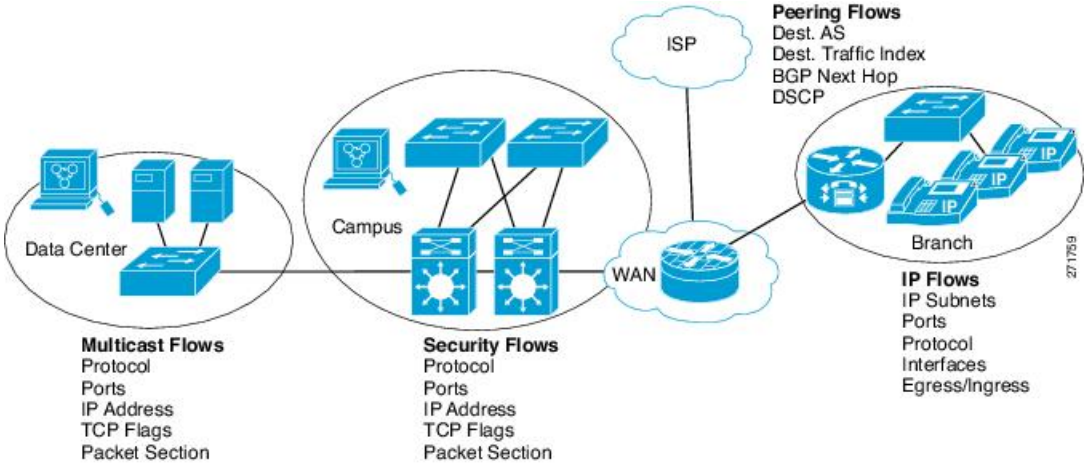
- スケーラビリティ、フロー情報の集約などの、大容量フロー認識。
- セキュリティの監視と dDoS の検出および識別のための拡張されたフローインフラストラクチャ。
- フロー情報をネットワーク内の特定のサービスまたはオペレーションに適応させるパケットからの新しい情報。利用できるフロー情報は、Flexible NetFlow ユーザがカスタマイズ可能。
- Cisco の柔軟で拡張可能な NetFlow Version 9 および Version 10 エクスポート フォーマットの活用。
- IP アカウンティング、ボーダー ゲートウェイ プロトコル（BGP）ポリシー アカウンティング、永続的キャッシュなどの多数のアカウンティング機能を置換するために使用できる包括的な IP アカウンティング機能。
- NetFlow の入出力アカウンティングのサポート。
- フロー アカウンティングのフル サポートおよびサンプリングした NetFlow アカウンティングのサポート。

Flexible NetFlow では、ネットワークの動作を、ネットワーク内で使用されるさまざまなサービスに合わせた特定のフロー情報とともに、より効率的に理解できます。次に、Flexible NetFlow 機能用の適用例を示します。

- Flexible NetFlow は Cisco NetFlow をセキュリティ監視ツールとして拡張します。たとえば、ユーザがネットワーク内で特定のタイプの攻撃を検索できるように、パケット長や MAC アドレスのために新しいフロー キーを定義することができます。
- Flexible NetFlow を使用すると、TCP アプリケーションまたは UDP アプリケーションをパケット内のサービス クラス（CoS）ごとに明確に追跡することによって、ホスト間で送信されるアプリケーション トラフィックの量を迅速に識別できます。
- サービス クラスごとに各ネクストホップのマルチプロトコル ラベル スイッチング（MPLS）か IP コア ネットワーク、およびその宛先を入力するトラフィックのアカウンティング。この機能では、エッジ間のトラフィック マトリクスを構築できます。

次の表に、Flexible NetFlow をネットワークに導入する方法の例を示します。

図 *1 : Flexible NetFlow* の通常の導入



Flexible NetFlow のコンポーネント

Flexible NetFlow は、いくつかのバリエーションで一緒に使用して、トラフィック分析およびデータ エクスポートに使用できるコンポーネントで構成されます。Flexible NetFlow のユーザ定義のフロー レコードおよびコンポーネントの構造では、最小限の数のコンフィギュレーション コマンドで、ネットワーキング デバイスでのトラフィック分析およびデータ エクスポートのためのさまざまなコンフィギュレーションの作成が容易になります。各フロー モニタに、フロー レコード、フロー エクスポータ、およびキャッシュ タイプの固有の組み合わせを設定できます。フロー エクスポータの宛先 IP アドレスなどのパラメータを変更する場合、フロー エクスポータを使用するすべてのフロー モニタに対して自動的に変更されます。同じフロー モニタを複数のフローサンプラと組み合わると、さまざまなインターフェイス上でさまざな速度の同じタイプのネットワーク トラフィックをサンプリングできます。ここでは、Flexible NetFlow コンポーネントのその他の情報を提供します。

フロー レコード

Flexible NetFlow では、キー フィールドと非キー フィールドの組み合わせをレコードと呼びます。Flexible NetFlow のレコードは Flexible NetFlow フロー モニタに割り当てられ、フロー データの格納に使用されるキャッシュが定義されます。

フローレコードでは、フロー内のパケットを識別するために Flexible NetFlow で使用するキーとともに、Flexible NetFlow がフローについて収集する他の関連フィールドを定義します。キーと関連フィールドを任意の組み合わせで指定して、フローレコードを定義できます。デバイスは、幅広いキーセットをサポートします。フローレコードでは、フロー単位で収集するカウンタのタイプも定義します。64 ビットのパケットまたはバイトカウンタを設定できます。デバイスは、フローレコードの作成時に、デフォルトとして次の match フィールドを有効にします。

- **match datalink**— レイヤ 2 属性
- **match flow direction**— フローの方向を識別するフィールドとの一致を指定します。
- **match interface**— インターフェイス属性
- **match ipv4**— IPv4 属性
- **match ipv6**— IPv6 属性
- **match transport**：トランスポート層フィールド
- **match flow cts**— Cisco TrustSec フィールド

ユーザ定義レコード

Flexible NetFlow では、key および nonkey フィールドを指定し、実際の要件に合わせてデータ収集をカスタマイズすることで、Flexible NetFlow フロー モニタ キャッシュ用の独自のレコードを定義できます。Flexible NetFlow フロー モニタ キャッシュに対して独自のレコードを定義する場合、ユーザ定義レコードと呼ばれます。nonkey フィールドの値は、フロー内のトラフィックに関する追加情報を提供するためにフローに追加されます。nonkey フィールドの値の変更によって新しいフローが作成されることはありません。ほとんどの場合、nonkey フィールドの値はフロー内の最初のパケットからのみ取得されます。Flexible NetFlow を使用すると、nonkey フィールドとして、フロー内のバイト数やパケット数などのカウンター値をキャプチャできます。

ユーザ定義レコードは、QoS および帯域幅監視、アプリケーションとユーザのトラフィック プロファイリング、dDoS 攻撃に対するセキュリティ監視などのアプリケーション用に作成できます。Flexible NetFlow のユーザ定義レコードでは、ユーザが設定可能なサイズのパケットの連続するセクションを監視する機能を利用でき、key フィールドまたは nonkey フィールドとしてパケットのその他のフィールドや属性とともにフロー レコード内で使用します。セクションにはパケットのレイヤ 3 データが含まれる場合があります。パケットフィールドの分析機能によって、さらに詳細なトラフィック監視が可能になるため、dDoS 攻撃の調査に役立ち、URL 監視など他のセキュリティ アプリケーションの実装が可能になります。

bytes 値は、フロー レコードのこれらのフィールドのサイズ（バイト単位）です。パケットの対応フラグメントが要求されたセクション サイズよりも小さい場合、Flexible NetFlow はフロー

レコード内の残りのセクション フィールドを 0 で埋めます。パケット タイプが要求されたセクション タイプと一致しなかった場合、Flexible NetFlow はフロー レコード内のセクション フィールド全体を 0 で埋めます。

Flexible NetFlow では、ヘッダーおよびパケット セクションのタイプに新しいバージョン 9 エクスポート フォーマット フィールド タイプが追加されます。Flexible NetFlow は NetFlow コレクタに、対応するバージョン 9 エクスポート テンプレート フィールドで設定されたセクション サイズを通知します。ペイロード セクションには、対応する長さフィールドがあり、収集されるセクションの実際のサイズを収集するために使用できます。

Flexible NetFlow の match パラメータ

次の表で、Flexible NetFlow の match パラメータについて説明します。フロー レコードごとに、次の match パラメータを 1 つ以上設定する必要があります。

表 *1 : match* パラメータ

コマンド	目的
match datalink {**dot1q** | **ethertype** | **mac** | **vlan** }	データ リンクまたはレイヤ 2 フィールドとの一致を指定します。次のコマンド オプションが使用可能です。 • **dot1q**：dot1q フィールドと一致します。 • **ethertype**：パケットの ethertype と一致します。 • **mac**：送信元または宛先の MAC フィールドと一致します。 • **vlan**：パケットが配置される VLAN と一致します（入力または出力）。
match flow direction	フローを識別するフィールドとの一致を指定します。
match interface {**input** | **output**}	インターフェイス フィールドとの一致を指定します。次のコマンド オプションが使用可能です。 • **input**：入力インターフェイスと一致します。 • **output**：出力インターフェイスと一致します。

コマンド	目的
match ipv4 {**destination** | **protocol** | **source** | **tos** | **ttl** | **version**}	IPv4 フィールドとの一致を指定します。次のコマンド オプションが使用可能です。 • **destination**：IPv4 宛先アドレス ベースのフィールドと一致します。 • **protocol**：IPv4 プロトコルと一致します。 • **source**：IPv4 送信元アドレス ベースのフィールドと一致します。 • **tos**：IPv4 タイプ オブ サービス フィールドと一致します。 • **ttl**：IPv4 存続時間フィールドと一致します。 • **version**：IPv4 ヘッダーの IP バージョンと一致します。
match ipv6 {**destination** | **hop-limit** | **protocol** | **source** | **traffic-class** | **version** }	IPv6 フィールドとの一致を指定します。次のコマンド オプションが使用可能です。 • **destination**：IPv6 宛先アドレス ベースのフィールドと一致します。 • **hop-limit**：IPv6 ホップ リミット フィールドと一致します。 • **protocol**：IPv6 ペイロード プロトコル フィールドと一致します。 • **source**：IPv6 送信元アドレス ベースのフィールドと一致します。 • **traffic-class**：IPv6 トラフィック クラスと一致します。 • **version**：IPv6 ヘッダーの IP バージョンと一致します。

コマンド	目的
match transport {**destination-port** | **igmp** | **icmp** | **source-port**}	トランスポート層フィールドとの一致を指定します。次のコマンド オプションが使用可能です。 • **destination-port**：転送先ポートと一致します。 • **icmp**：ICMP IPv4 および IPv6 フィールドを含む ICMP フィールドと一致します。 • **igmp**：IGMP フィールドと一致します。 • **source-port**：転送元ポートと一致します。

Flexible NetFlow の collect パラメータ

次の表で、Flexible NetFlow の collect パラメータについて説明します。

表 *2 : collect* パラメータ

コマンド	目的
collect counter { **bytes** { **layer2** { **long** } | **long** } | **packets** { **long** } }	カウンタ フィールドの合計バイト数と合計パケット数を収集します。
collect interface {**input** | **output**}	入力または出力インターフェイスからフィールドを収集します。
collect timestamp absolute {**first** | **last**}	最初のパケットが確認された絶対時間、または最新のパケットが最後に確認された絶対時間のフィールドを収集します（ミリ秒）。

コマンド	目的
collect transport tcp flags	次の転送 TCP フラグを収集します。 • **ack**：TCP 確認応答フラグ • **cwr**：TCP 輻輳ウィンドウ縮小フラグ • **ece**：TCP ECN エコー フラグ • **fin**：TCP 終了フラグ • **psh**：TCP プッシュ フラグ • **rst**：TCP リセット フラグ • **syn**：TCP 同期フラグ • **urg**：TCP 緊急フラグ （注） デバイスでは、収集する TCP フラグを指定できません。転送 TCP フラグの収集のみ指定できます。すべての TCP フラグはこのコマンドで収集されます。
collect counter bytes	フローの確認されたバイト数を非キー フィールドとして設定し、フローの合計バイト数を収集します。
collect counter packets	フローで確認されるパケット数を非キーフィールドとして設定し、フローから合計パケット数を収集します。

フロー エクスポータ

フローエクスポータでは、フロー モニタ キャッシュ内のデータをリモートシステム（たとえば、分析および保管のために NetFlow コレクタを実行するサーバ）にエクスポートします。フローエクスポータは、コンフィギュレーションで別のエンティティとして作成されます。フローエクスポータは、フローモニタにデータエクスポート機能を提供するためにフローモニタに割り当てられます。複数のフローエクスポータを作成して、1 つまたは複数のフローモニタに適用すると、いくつかのエクスポート先を指定することができます。1つのフローエクスポータを作成し、いくつかのフローモニタに適用することができます。

NetFlow データ エクスポート フォーマット バージョン 10（IPFIX）

Internet Protocol Flow Information Export（IPFIX）、つまりバージョン 10 は、またはユーザ定義のフロー レコードを収集し、エクスポートするエクスポート プロトコルです。IPFIX は NetFlow バージョン 9に基づいた IETF 標準です。IPFIX 形式は NetFlow バージョン 9 として、個別のテ

ンプレートとレコードについて同じ原則を保ちます。IPFIXエクスポートプロトコルでは、デフォルトの宛先ポートは 4739、DSCP 値は 0、TTL は 255 です。

NetFlow データ エクスポート フォーマットのバージョン 9

NetFlow の基本出力はフロー レコードです。NetFlow が改良され、フロー レコードのいくつかのフォーマットが向上しました。NetFlow エクスポート フォーマットの最新の進化は、バージョン 9 と呼ばれます。NetFlow Version 9 エクスポート フォーマットの識別機能は、テンプレートがベースとなります。テンプレートは、レコードフォーマットの設計を拡張可能なものにします。NetFlowサービスが将来拡張されても、基本フロー レコードフォーマットを変更し続ける必要がありません。テンプレートを使用すると、次のいくつかの利点があります。

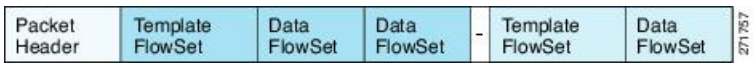
- NetFlow のコレクタを提供したり、サービスを表示したりするアプリケーションを作成するサードパーティ ビジネス パートナーは、新規の NetFlow 機能が追加されるたびにアプリケーションを再コンパイルする必要はありません。代わりに、既知のテンプレートフォーマットを記述する外部のデータ ファイルを使用することができます。
- 新規機能は、現在の導入環境を損ねることなく、NetFlow に迅速に追加できます。
- バージョン9フォーマットは新しいプロトコルや開発中のプロトコルに適応できるため、NetFlow はこれらのプロトコルに対して「将来的に対応」します。

NetFlow バージョン 9 エクスポート フォーマットは、次の特徴と機能を提供します。

- 可変フィールド仕様フォーマット
- IPv4 または IPv6 の宛先アドレスのエクスポートのサポート
- ネットワークをより効率的に利用可能

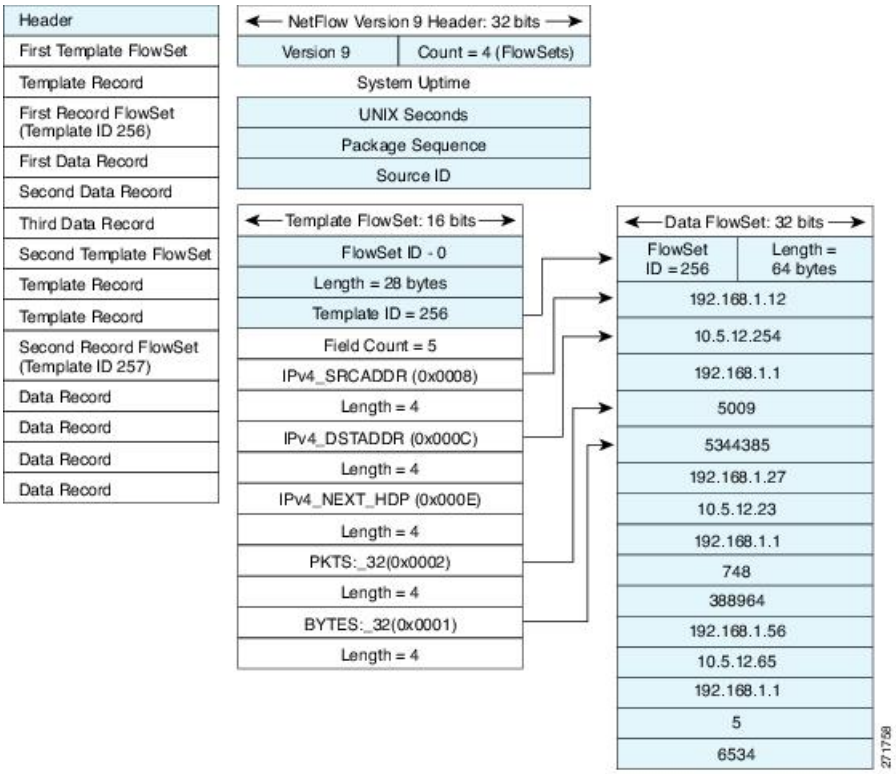
バージョン 9 のエクスポート フォーマットは、パケット ヘッダーとそれに続く 1 つ以上のテンプレート フロー セットまたはデータ フロー セットで構成されています。テンプレート フローセットでは、将来のデータ フローセットに表示されるフィールドの説明が提供されます。このようなデータ フロー セットは、後で同じエクスポート パケットまたは後続のエクスポート パケットで発生する可能性があります。テンプレート フロー セットおよびデータ フロー セットは、次の図に示すように、単一のエクスポート パケットに混在させることができます。

図 *2:* バージョン *9* エクスポート パケット



NetFlow Version 9 では、送信されるデータを NetFlow コレクタが理解できるように、テンプレート データを定期的にエクスポートします。また、テンプレートのデータ フロー セットもエクスポートします。Flexible NetFlow の主な利点は、ユーザがフロー レコードを設定すると、バージョン9テンプレートに効率的に変換され、コレクタに転送されることです。下の図に、ヘッダー、テンプレート フロー セットおよびデータ フロー セットを含めて、NetFlow Version 9 エクスポート フォーマットの詳細な例を示します。

図 *3 : NetFlow* バージョン *9* エクスポート フォーマットの詳細例



バージョン 9 エクスポート フォーマットの詳細については、ホワイト ペーパー『Cisco IOS NetFlow Version 9 Flow-Record Format』を参照してください。次の URL から入手できます。http://www.cisco.com/en/US/tech/tk648/tk362/technologies_white_paper09186a00800a3db9.shtml

フロー モニタ

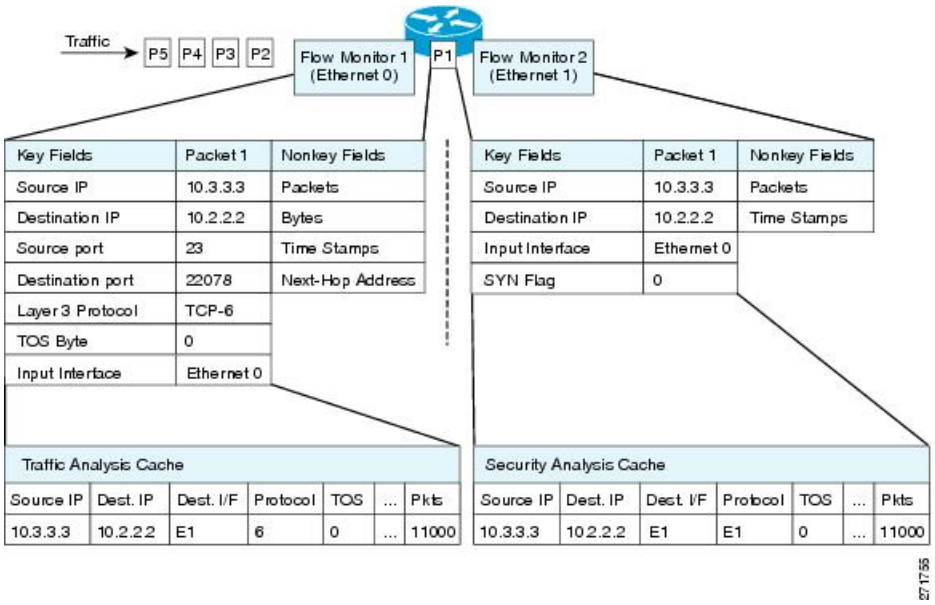
フロー モニタは Flexible NetFlow のネットワーク トラフィックの監視を実行するコンポーネントで、インターフェイスに適用されます。

フロー モニタは、ユーザ定義のレコード、オプションのフロー エクスポータ、およびフロー モニタが最初のインターフェイスに適用されるときに自動的に作成されるキャッシュで構成されます。

フロー データはネットワーク トラフィックから収集され、フロー レコードの key フィールドおよび nonkey フィールドに基づいて監視プロセス中にフロー モニタ キャッシュに追加されます。

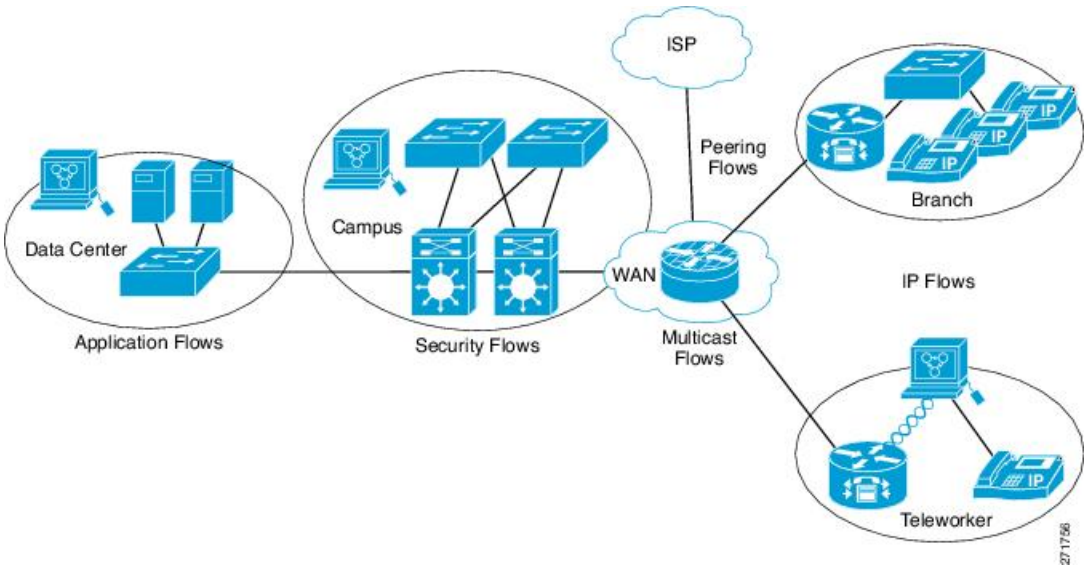
Flexible NetFlow は、同じトラフィックのさまざまなタイプの分析を実行するために使用できます。下の図では、入力インターフェイス上の標準トラフィック分析のために設計されたレコードと、出力インターフェイス上のセキュリティ分析のために設計されたレコードを使用してパケット 1 が分析されます。

図 *4: 2*つのフロー モニタを使用した同じトラフィックの分析例



下の図に、カスタム レコードを使用して複数のタイプのフロー モニタを適用するより複雑な方法の例を示します。

図 *5:* カスタム レコードでの複数のタイプのフロー モニタの複雑な使用例



標準

デフォルトのキャッシュ タイプは「normal」です。このモードでは、キャッシュ内のエントリが timeout active 設定と timeout inactive 設定に従って期限切れになります。キャッシュ エントリは、期限切れになるとキャッシュから削除され、設定されている何らかのエクスポータによってエクスポートされます。

フロー サンプラー

フローサンプラーは、ルータのコンフィギュレーションで別のコンポーネントとして作成されます。フローサンプラは、分析用に選択されるパケットの数を制限することで、FlexibleNetFlowを実行しているデバイス上の負荷を減らすために使用されます。

フロー サンプリングでは、ルータのパフォーマンスに対するモニタリング精度が交換されます。サンプラーをフロー モニタに適用すると、フロー モニタが分析する必要のあるパケット数が減少するため、ルータでフロー モニタを実行するためのオーバーヘッド負荷が低下します。フロー モニタで分析されるパケット数が減少すると、フロー モニタのキャッシュに格納される情報の精度が、それに応じて低下します。

ip flow monitor コマンドを使用してインターフェイスに適用される場合、サンプラーはフローモニタと組み合わせて使用されます。

サポートされている Flexible NetFlow フィールド

次の表では、さまざまなトラフィック タイプおよびトラフィック方向について、FlexibleNetFlow（FNF）でサポートされるフィールドの統合リストを提供しています。

（注） パケットに VLAN フィールドがある場合、その長さは考慮されません。

フィールド	レイヤ 2 In	レイヤ 2 Out	IPv4 In	IPV4 Out	IPv6 In	IPv6 Out	注意
Key または Collect フィールド							

フィールド	レイヤ 2 In	レイヤ 2 Out	IPv4 In	IPV4 Out	IPv6 In	IPv6 Out	注意
インターフェイス入力	対応	—	対応	—	対応	—	フロー モニタを入力方向に適用する場合： • **match** キーワードを使用し、入力インターフェイスを key フィールドとして使用します。 • **collect** キーワードを使用し、出力インターフェイスを collect フィールドとして使用します。このフィールドはエクスポートされるレコードに含まれますが、値は 0 になります。
インターフェイス出力	—	対応	—	対応	—	対応	フロー モニタを出力方向に適用する場合： • **match** キーワードを使用し、出力インターフェイスを key フィールドとして使用します。 • **collect** キーワードを使用し、入力インターフェイスを collect フィールドとして使用します。このフィールドはエクスポートされるレコードに含まれますが、値は 0 になります。

フィールド	レイヤ 2 In	レイヤ 2 Out	IPv4 In	IPV4 Out	IPv6 In	IPv6 Out	注意
Key フィールド							

フィールド	レイヤ 2 In	レイヤ 2 Out	IPv4 In	IPV4 Out	IPv6 In	IPv6 Out	注意
フロー方向	対応	対応	対応	対応	対応	対応	
Ethertype	対応	対応	—	—	—	—	
VLAN 入力	対応	—	対応	—	対応	—	スイッチポートでのみサポートされています。
VLAN 出力	—	対応	—	対応	—	対応	スイッチポートでのみサポートされています。
dot1q VLAN 入力	対応	—	対応	—	対応	—	スイッチポートでのみサポートされています。
dot1q VLAN 出力	—	対応	—	対応	—	対応	スイッチポートでのみサポートされています。
dot1q 優先度	対応	対応	対応	対応	対応	対応	スイッチポートでのみサポートされています。
MAC 送信元アドレス入力	対応	対応	対応	対応	対応	対応	

フィールド	レイヤ 2 In	レイヤ 2 Out	IPv4 In	IPV4 Out	IPv6 In	IPv6 Out	注意
MAC 送信元アドレス出力	—	—	—	—	—	—	
MAC 宛先アドレス入力	対応	—	対応	—	対応	—	
MAC 送信先アドレス出力	—	対応	—	対応	—	対応	
IPv4 バージョン	—	—	対応	対応	対応	対応	
IPv4 TOS	—	—	対応	対応	対応	対応	
IPv4 プロトコル	—	—	対応	対応	対応	対応	送信元/宛先ポート、ICMP コード/タイプ、IGMP タイプ、TCP フラグのいずれかが使用されている場合に使用する必要があります。
IPv4 TTL	—	—	対応	対応	対応	対応	
IPv4 TTL	—	—	対応	対応	対応	対応	IPv4 TTL と同じです。

フィールド	レイヤ 2 In	レイヤ 2 Out	IPv4 In	IPV4 Out	IPv6 In	IPv6 Out	注意
IPv4 プロトコル	—	—	対応	対応	対応	対応	IPv4 プロトコルと同じです。送信元/宛先ポート、ICMP コード/タイプ、IGMP タイプ、TCP フラグのいずれかが使用されている場合に使用する必要があります。
IPv4 発信元アドレス	—	—	対応	対応	—	—	
IPv4 宛先アドレス	—	—	対応	対応	—	—	
ICMP IPv4 タイプ	—	—	対応	対応	—	—	
ICMP IPv4 コード	—	—	対応	対応	—	—	
IGMP タイプ	—	—	対応	対応	—	—	

フィールド	レイヤ 2 In	レイヤ 2 Out	IPv4 In	IPV4 Out	IPv6 In	IPv6 Out	注意
Key フィールド（続き）							

フィールド	レイヤ 2 In	レイヤ 2 Out	IPv4 In	IPV4 Out	IPv6 In	IPv6 Out	注意
IPv6 バージョン	—	—	対応	対応	対応	対応	IP バージョンと同じです。
IPv6 プロトコル	—	—	対応	対応	対応	対応	IP プロトコルと同じです。送信元/宛先ポート、ICMP コード/タイプ、IGMP タイプ、TCP フラグのいずれかが使用されている場合に使用する必要があります。
IPv6 送信元アドレス	—	—	—	—	対応	対応	
IPv6 宛先アドレス	—	—	—	—	対応	対応	
IPv6 トラフィッククラス	—	—	対応	対応	対応	対応	IP TOS と同じです。
IPv6 ホップ リミット	—	—	対応	対応	対応	対応	IP TTL と同じです。
ICMP IPv6 タイプ	—	—	—	—	対応	対応	
ICMP IPv6 コード	—	—	—	—	対応	対応	

フィールド	レイヤ 2 In	レイヤ 2 Out	IPv4 In	IPV4 Out	IPv6 In	IPv6 Out	注意
source-port	—	—	対応	対応	対応	対応	
dest-port	—	—	対応	対応	対応	対応	

フィールド	レイヤ 2 In	レイヤ 2 Out	IPv4 In	IPV4 Out	IPv6 In	IPv6 Out	注意
Collect フィールド							
バイト長	対応	対応	対応	対応	対応	対応	パケットサイズ =（FCS を含むイーサネットフレームサイズ - 18 バイト） **推奨**： このフィールドを回避し、Bytes layer2 long を使用します。
パケット長	対応	対応	対応	対応	対応	対応	
Timestamp absolute first	対応	対応	対応	対応	対応	対応	
Timestamp absolute last	対応	対応	対応	対応	対応	対応	
TCP フラグ	対応	対応	対応	対応	対応	対応	すべてのフラグを収集します。

フィールド	レイヤ 2 In	レイヤ 2 Out	IPv4 In	IPV4 Out	IPv6 In	IPv6 Out	注意
Bytes layer2 long	対応	対応	対応	対応	対応	対応	

デフォルト設定

次の表は、デバイスに対する Flexible NetFlow のデフォルト設定を示します。

表 *3:* デフォルトの *Flexible NetFlow* 設定

設定	デフォルト
フロー アクティブ タイムアウト	1800 秒
フロー タイムアウトの非アクティブ化	15 秒

Autonomous System Number

自律システム番号スペースは、4,294,967,296 個の一意の値を持つ 32 ビットのフィールドで、インターネットのパブリック ドメイン間ルーティング システムをサポートするために使用できます。

自律システム番号（AS 番号）は、主にボーダー ゲートウェイ プロトコルで使用される IANA によって割り当てられる特別な番号です。一意のルーティング ポリシーを持つ単一の技術管理下にあるネットワーク、またはパブリック インターネットにマルチホーム接続されているネットワークを一意に識別します。この自律システム番号は、ピアリング ポイントのインターネット サービス プロバイダーとインターネット エクスチェンジ（IX）の間で、BGP およびピアをインターネット サービス プロバイダーと実行するために必要です。AS 番号はグローバルに一意である必要があります。これにより、BGP が検出してルーティングできる一意の場所から IP アドレス ブロックが送信されるようになります。BGP は、プレフィックスと自律システム パス（AS パス）を使用して、プレフィックスが存在する宛先への最短パスを決定します。

NetFlow V9 および IPFIX エクスポート タイプは、32 ビット AS 番号をサポートします。NetFlow V5 は、固定 16 ビットの送信元および宛先 AS 形式に従うため、この 32 AS フィールドをサポートしません。

NetFlow では、次の BGP パラメータをエクスポートできます。

- BGP 送信元起源またはピア AS 番号
- BGP 宛先起源またはピア AS 番号

設定

AS 番号システムを設定するには、次のコマンドを使用します。

[no] collect routing { **destination | source** } as **[[4-octet] peer] [4-octet]**

MPLS での入出力 Flexible NetFlow の概要

- MPLS での入力 Flexible NetFlow（IP レベル）：この機能を使用すると、MPLS ラベルインポジションを経て MPLS ネットワークに入るパケットのインターネットプロトコル（IP）フロー情報をキャプチャできます。これらのパケットは、IP パケットとしてルータに到着し、MPLS パケットとして送信されます。PE ノードの CE 側に IPv4 および IPv6 トラフィックの入力フローモニタを設定することにより、この機能を有効にできます。
- MPLS での出力 Flexible NetFlow（IP レベル）：この機能を使用すると、MPLS ラベルインポジションを経て MPLS ネットワークから出るパケットのインターネットプロトコル（IP）フロー情報をキャプチャできます。これらのパケットは、MPLS パケットとしてルータに到着し、IP パケットとして送信されます。PE ノードの CE 側に IPv4 および IPv6 トラフィックの出力フローモニタを設定することにより、この機能を有効にできます。

Flexible NetFlow の VPN ID の設定

同じプライベートネットワークからの複数の VPN は、データトラフィックで同じプライベート送信元および宛先 IP を使用できます。これにより、データが属する IP アドレスを特定することが困難になる可能性があります。VPN-ID を使用してこの問題を解決できます。VPN-ID は、グローバルに一意の仮想プライベートネットワーク識別子です。自律システム（AS）全体で VPN を識別するために使用されます。VPN-ID が NetFlow エクスポートパケットでエクスポートされる場合、別の AS のコレクタは、データが属する VPN に基づいてフローを関連付けて分離できます。VPN-ID は VRF-ID と同様のシステムレベルプロパティであり、同様の方法でエクスポートできます。

VPN ID の構成要素

各 VPN ID は次の要素で構成されています。

- 3 オクテットの 16 進数である組織固有識別子（OUI）。IEEE 登録局は、ISO/IEC 8802 規格の下でコンポーネントを製造するあらゆる企業に OUI を割り当てます。OUI は、ローカル エリア ネットワーク アプリケーションとメトロポリタン エリア ネットワーク アプリケーションで使用するための、汎用的な LAN MAC アドレスとプロトコル ID を生成するために使用されます。たとえば、Cisco Systems の OUI は 00-03-6B（16 進数）です。
- 企業内での VPN を示す 4 オクテットの 16 進数である VPN インデックス。

VRF 定義コンフィギュレーション モードで **vpn id** コマンドを使用して、VPN ID を設定できます。VPN ID を次の形式で指定します。

vpn id oui:vpn-index

VPN ID を設定したら、flow-exporter コンフィギュレーション モードで **option vrf-attributes** コマンドを使用して VPN ID を設定できます。

Flexible NetFlow の設定方法

Flexible Netflow を設定するには、次の一般的な手順に従います。

1. フローにキー フィールドおよび非キー フィールドを指定して、フロー レコードを作成します。
2. プロトコルを指定して任意のフローエクスポータを作成し、宛先ポート、宛先、およびその他のパラメータを転送します。
3. フロー レコードおよびフロー エクスポータに基づいて、フロー モニタを作成します。
4. 任意のサンプラーを作成します。
5. レイヤ 2 ポート、レイヤ 3 ポート、または VLAN にフロー モニタを適用します。

フロー レコードの作成

カスタマイズしたフロー レコードを設定するには、次のタスクを実行します。

カスタマイズしたフロー レコードは、特定の目的でトラフィック データを分析するために使用します。カスタマイズしたフローレコードには、key フィールドとして使用する **match** 基準が 1 つ以上必要です。通常は nonkey フィールドとして使用する **collect** 基準が 1 つ以上あります。

カスタマイズしたフロー レコードの順列は、数百もの可能性があります。このタスクでは、可能性のある順列の 1 つを作成するための手順について説明します。必要に応じて当該タスクの手順を変更し、要件に合わせてカスタマイズしたフロー レコードを作成します。

手順の概要

1. **enable**
2. **configure terminal**
3. **flow record** *record-name*
4. **description** *description*
5. **match** {**ip** | **ipv6**} {**destination** | **source**} **address**
6. 必要に応じてステップ 5 を繰り返し、レコードの追加 key フィールドを設定します。
7. **match flow cts** {**source** | **destination**} **group-tag**
8. **end**
9. **show flow record** *record-name*
10. **show running-config flow record** *record-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**flow record** *record-name* 例： `Device(config)# flow record FLOW-RECORD-1`	フロー レコードを作成し、Flexible NetFlow フロー レコード コンフィギュレーション モードを開始します。 • このコマンドでは、既存のフロー レコードを変更することもできます。
ステップ 4	**description** *description* 例： `Device(config-flow-record)# description Used for basic traffic analysis`	（任意）フロー レコードの説明を作成します。
ステップ 5	**match** {**ip** | **ipv6**} {**destination** | **source**} **address** 例： `Device(config-flow-record)# match ipv4 destination address`	（注） この例では、IPv4 宛先アドレスをレコードの key フィールドとして設定します。
ステップ 6	必要に応じてステップ 5 を繰り返し、レコードの追加 key フィールドを設定します。	—

ステップ 7	**match flow cts** {**source** | **destination**} **group-tag**
	例：
	`Device(config-flow-record)# match flow cts source group-tag`
	`Device(config-flow-record)# match flow cts destination group-tag`
		（注） この例では、CTS の送信元グループ タグと宛先グループ タグをレコードのキー フィールドとして設定します。**match ipv4**/**ipv6** コマンドで利用できるその他の key フィールド、および key フィールドの設定に利用できる他の **match** コマンドの詳細について。

	コマンドまたはアクション	目的
		（注） • 出力： • SGT または CTS のいずれかの伝播が出力インターフェイス上で無効化されていると、SGT は 0 になります。 • 発信パケットで、（SGT、DGT）に対応する SGACL 設定が存在すれば、DGT はゼロ以外になります。 • SGACL が出力ポート/VLANで無効化されているか、またはグローバル SGACL の強制を無効化されている場合、DGT は 0 になります。 • 入力： • 着信パケットでは、ヘッダーがある場合、SGT にはヘッダーと同じ値が反映されます。値がない場合は、0 が示されます。 • DGT 値は入力ポートの SGACL 設定に依存しません。
ステップ 8	**end** 例： `Device(config-flow-record)# end`	Flexible NetFlow フロー レコード コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 9	**show flow record** *record-name* 例： `Device# show flow record FLOW_RECORD-1`	（任意）指定したフロー レコードの現在のステータスが表示されます。
ステップ 10	**show running-config flow record** *record-name* 例： `Device# show running-config flow record FLOW_RECORD-1`	（任意）指定したフロー レコードの設定が表示されます。

フロー エクスポータの作成

フロー エクスポートを作成して、フローのエクスポート パラメータを定義できます。

（注） フローエクスポータごとに、1 つ宛先のみがサポートされます。複数の宛先にデータをエクスポートする場合は、複数のフロー エクスポータを設定してフロー モニタに割り当てる必要があります。

IPv4 または IPv6 アドレスを使用して宛先にエクスポートできます。

手順の概要

1. **enable**
2. **configure terminal**
3. **flow exporter** *name*
4. **description** *string*
5. **destination** {*ipv4-address*| *ipv6-address*}
6. **dscp** *value*
7. **source** *interface type interface number*
8. **transport udp** *number*
9. **ttl** *seconds*
10. **export-protocol** {**netflow-v9** | **ipfix**}
11. **end**
12. **show flow exporter** [**name** *record-name*]
13. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device(config)# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**flow exporter** *name* 例： `Device(config)# flow exporter ExportTest`	フロー エクスポータを作成し、フロー エクスポータ コンフィギュレーション モードを開始します。このコマンドを使用して既存のフロー エクスポータを変更することもできます。

	コマンドまたはアクション	目的
ステップ 4	**description** *string* 例： `Device(config-flow-exporter)# description ExportV9`	（任意）最大 63 文字で、このフローの説明を指定します。
ステップ 5	**destination** {*ipv4-address*| *ipv6-address*} 例： `Device(config-flow-exporter)# destination 192.0.2.1 (IPv4 destination)`	このエクスポータに IPv4/IPv6 宛先アドレスまたはホスト名を設定します。
ステップ 6	**dscp** *value* 例： `Device(config-flow-exporter)# dscp 0`	（任意）DSCP（DiffServ コードポイント）値を指定します。範囲は 0 ～ 63 です。デフォルトは 0 です。
ステップ 7	**source** *interface type interface number* 例： `Device(config-flow-exporter)# source gigabitEthernet1/0/1`	（任意）設定された宛先で NetFlow コネクタに到達するために使用するインターフェイスを指定します。 （注） フローエクスポータは、送信元インターフェイスとしてアンナンバード IP インターフェイスをサポートしていません。 送信元として次のインターフェイスを設定できます。 • **Auto Template**：自動テンプレート インターフェイス • **Capwap**：Capwap トンネル インターフェイス • **GigabitEthernet**：Gigabit Ethernet IEEE 802 • **GroupVI**：グループ仮想インターフェイス • **Internal Interface**：内部インターフェイス • **Loopback**：ループバック インターフェイス • **Null**：ヌル インターフェイス • **Port-channel**：インターフェイスのイーサネット チャネル

	コマンドまたはアクション	目的
		• **TenGigabitEthernet**：10 ギガビット イーサネット • **Tunnel**：トンネル インターフェイス • **Vlan**：Catalyst VLAN
ステップ 8	**transport udp** *number* 例： `Device(config-flow-exporter)# transport udp 200`	（任意）NetFlow コレクタに到達するために使用する UDP ポートを指定します。範囲は 0 ～ 65535 です。プロトコルをエクスポートする IPFIX の場合、デフォルトの宛先ポートは 4739 です。
ステップ 9	**ttl** *seconds* 例： `Device(config-flow-exporter)# ttl 210`	（任意）エクスポータによって送信されるデータグラムの存続可能時間（TTL）値を設定します。範囲は 1 ～ 255 秒です。デフォルトは 255 です。
ステップ 10	**export-protocol** {**netflow-v9** | **ipfix**} 例： `Device(config-flow-exporter)# export-protocol netflow-v9`	エクスポータで使用される NetFlow エクスポート プロトコルのバージョンを指定します。 • デフォルト：**netflow-v9**
ステップ 11	**end** 例： `Device(config-flow-record)# end`	特権 EXEC モードに戻ります。
ステップ 12	**show flow exporter** [**name** *record-name*] 例： `Device# show flow exporter ExportTest`	（任意）NetFlow のフロー エクスポータ情報を表示します。
ステップ 13	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

次のタスク

フロー レコードおよびフロー エクスポータに基づいて、フロー モニタを定義します。

カスタマイズしたフロー モニタの作成

カスタマイズしたフロー モニタを作成するには、この必須のタスクを実行します。

各フロー モニタには、専用のキャッシュが割り当てられています。フロー モニタごとに、キャッシュ エントリの内容およびレイアウトを定義するレコードが必要です。これらのレコード フォーマットは、事前定義済みのレコード フォーマットのいずれか、またはユーザ定義にすることができます。上級のユーザであれば **flow record** コマンドを使用して、カスタマイズしたフォーマットを作成することもできます。

始める前に

Flexible NetFlow の事前定義済みレコードの代わりにカスタマイズしたレコードを使用する場合は、このタスクを実行する前に、カスタマイズしたレコードを作成する必要があります。データをエクスポートするためにフロー エクスポータをフロー モニタに追加する場合は、このタスクを完了する前にエクスポータを作成する必要があります。

（注） フローモニタで **record** コマンドのパラメータを変更する前に、**no ip flow monitor** コマンドを使用して、すべてのインターフェイスから適用済みのフローモニタを削除する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **flow monitor** *monitor-name*
4. **description** *description*
5. **record** {*record-name* | **netflow-original** | **netflow** {**ipv4** | **ipv6**} *record* [**peer**]}
6. **cache** {**timeout** {**active** | **inactive** | **update**} *seconds* | **type normal** }
7. 必要に応じてステップ 6 を繰り返して、このフローモニタのキャッシュ パラメータの変更を完了します。
8. **statistics packet protocol**
9. **statistics packet size**
10. **exporter** *exporter-name*
11. **end**
12. **show flow monitor** [[**name**] *monitor-name* [**cache** [**format** {**csv** | **record** | **table**}]] [**statistics**]]
13. **show running-config flow monitor** *monitor-name*
14. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
	`Device> enable`	
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**flow monitor** *monitor-name* 例： `Device(config)# flow monitor FLOW-MONITOR-1`	フロー モニタを作成し、Flexible NetFlow フロー モニタ コンフィギュレーションモードを開始します。 • このコマンドでは、既存のフロー モニタを変更することもできます。
ステップ 4	**description** *description* 例： `Device(config-flow-monitor)# description Used for basic ipv4 traffic analysis`	（任意）フロー モニタの説明を作成します。
ステップ 5	**record** {*record-name* | **netflow-original** | **netflow** {**ipv4** | **ipv6**} *record* [**peer**]} 例： `Device(config-flow-monitor)# record FLOW-RECORD-1`	フロー モニタのレコードを指定します。

ステップ 6	**cache** {**timeout** {**active** | **inactive** | **update**} *seconds* | **type normal** }
	例：
	`Device(config-flow-monitor)# cache type normal`
	`Device(config-flow-monitor)# cache timeout active`
		（任意）フロー モニタ キャッシュ パラメータ（タイムアウト値、キャッシュタイプなど）を変更します。指定したフロー モニタとフロー キャッシュを関連付けます。

ステップ 7	必要に応じてステップ 6 を繰り返して、このフロー モニタのキャッシュ パラメータの変更を完了します。	—
ステップ 8	**statistics packet protocol** 例： `Device(config-flow-monitor)# statistics packet protocol`	（任意）Flexible NetFlow モニタのプロトコル分散統計情報の収集をイネーブルにします。
ステップ 9	**statistics packet size** 例： `Device(config-flow-monitor)# statistics packet size`	（任意）Flexible NetFlow モニタのサイズ分散統計情報の収集をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 10	**exporter** *exporter-name* 例： `Device(config-flow-monitor)# exporter EXPORTER-1`	（任意）事前に作成されたエクスポータの名前を指定します。
ステップ 11	**end** 例： `Device(config-flow-monitor)# end`	Flexible NetFlow フロー モニタ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 12	**show flow monitor** [[**name**] *monitor-name* [**cache** [**format** {**csv** | **record** | **table**}]] [**statistics**]] 例： `Device# show flow monitor FLOW-MONITOR-2 cache`	（任意）Flexible NetFlow フロー モニタのステータスおよび統計情報が表示されます。
ステップ 13	**show running-config flow monitor** *monitor-name* 例： `Device# show running-config flow monitor FLOW_MONITOR-1`	（任意）指定したフロー モニタの設定が表示されます。
ステップ 14	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

フローサンプラーの作成

フロー サンプラーを設定して有効化するには、この必須のタスクを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **sampler** *sampler-name*
4. **description** *description*
5. **mode** {**random**} **1 out-of** *window-size*
6. **exit**
7. **interface** *type number*
8. {**ip** | **ipv6**} **flow monitor** *monitor-name* [[**sampler**] *sampler-name*] {**input** | **output**}
9. **end**

10. **show sampler sampler-name**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**sampler** *sampler-name* 例： `Device(config)# sampler SAMPLER-1`	サンプラーを作成し、サンプラーコンフィギュレーション モードを開始します。 • このコマンドでは、既存のサンプラーを変更することもできます。
ステップ 4	**description** *description* 例： `Device(config-sampler)# description Sample at 50%`	（任意）フロー サンプラーの説明を作成します。
ステップ 5	**mode** {**random**} **1 out-of** *window-size* 例： `Device(config-sampler)# mode random 1 out-of 2`	サンプラー モードおよびフロー サンプラーのウィンドウ サイズを指定します。 • *window-size* 引数の範囲は、0 ～ 1024 です。
ステップ 6	**exit** 例： `Device(config-sampler)# exit`	サンプラー コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**interface** *type number* 例： `Device(config)# interface GigabitEthernet 0/0/0`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 8	{**ip** | **ipv6**} **flow monitor** *monitor-name* [[**sampler**] *sampler-name*] {**input** | **output**} 例： `Device(config-if)# ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 input`	作成したフロー モニタおよびフロー サンプラーをインターフェイスに割り当てて、サンプリングをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 9	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 10	**show sampler sampler-name** 例： `Device# show sampler SAMPLER-1`	設定し有効化したフロー サンプラーのステータスおよび統計情報を表示します。

インターフェイスへのフローの適用

フロー モニタおよびオプションのサンプラーをインターフェイスに適用できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type*
4. {**ip flow monitor** | **ipv6 flow monitor** | **datalink flow monitor**} *name* [**sampler** *name*] {**input** | **output**}
5. **end**
6. **show flow interface** [*interface-type number*]
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device(config)# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type* 例： `Device(config)# interface GigabitEthernet1/0/1`	インターフェイス コンフィギュレーション モードを開始し、インターフェイスを設定します。 FlexibleNetFlowは、L2ポートチャネルインターフェイスではサポートされませんが、L2ポートチャネルメンバー ポートではサポートされます。

	コマンドまたはアクション	目的
		Flexible NetFlow は、L3 ポートチャネル インターフェイスとメンバポートでサポートされますが、両方に対して同時にサポートされることはありません。 インターフェイス コンフィギュレーションのコマンド パラメータは次のとおりです。 • **GigabitEthernet**：GigabitEthernet IEEE 802 • **Loopback**：ループバック インターフェイス • **TenGigabitEthernet**：10 ギガビット イーサネット • **Vlan**：Catalyst VLAN • **Range**：インターフェイス範囲
ステップ 4	{**ip flow monitor** | **ipv6 flow monitor** | **datalink flow monitor**} *name* [**sampler** *name*] {**input** | **output**} 例： `Device(config-if)# ip flow monitor MonitorTest input`	入力または出力パケットに対応するインターフェイスに、IPv4、IPv6、データリンクフローモニタ、およびオプションのサンプラーを関連付けます。 **ip flow monitor** – Flexible NetFlow で IPv4 トラフィックを監視できます。 **ipv6 flow monitor** – Flexible NetFlow で IPv6 トラフィックを監視できます。 **datalink flow monitor** – Flexible NetFlow で非 IP のトラフィックを監視できます。 （注） 同じ方向のインターフェイスに、異なるトラフィック タイプの複数のモニタを関連付けることができます。ただし、同じ方向のインターフェイスに、同じトラフィック タイプの複数のモニタを関連付けることはできません。
ステップ 5	**end** 例： `Device(config-flow-monitor)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show flow interface** [*interface-type number*] 例： `Device# show flow interface`	（任意）インターフェイスの NetFlow 情報を表示します。

	コマンドまたはアクション	目的
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

VLAN 上でのブリッジ型 NetFlow の設定

フロー モニタおよびオプションのサンプラーを VLAN に適用できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **vlan** [**configuration**] *vlan-id*
4. **ip flow monitor** *monitor name* [**sampler** *sampler name*] { **input** | **output**}
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device(config)# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	**vlan** [**configuration**] *vlan-id*
	例：
	`Device(config)# vlan configuration 30`
	`Device(config-vlan-config)#`
		VLAN または VLAN コンフィギュレーション モードを開始します。

ステップ 4	**ip flow monitor** *monitor name* [**sampler** *sampler name*] { **input**	**output**} 例： `Device(config-vlan-config)# ip flow monitor MonitorTest input`	入力または出力パケットに対応する VLAN に、フローモニタおよびオプションのサンプラーを関連付けます。

	コマンドまたはアクション	目的
ステップ 5	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

レイヤ 2 NetFlow の設定

Flexible NetFlow レコード内でレイヤ 2 キーを定義できます。このレコードを使用して、レイヤ 2 インターフェイスのフローをキャプチャできます。

手順の概要

1. **enable**
2. **configure terminal**
3. **flow record** *name*
4. **match datalink** {**dot1q** |**ethertype** | **mac** | **vlan**}
5. **end**
6. **show flow record** [*name*]
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device(config)# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	**flow record** *name*
	例：
	`Device(config)# flow record L2_record`
	`Device(config-flow-record)#`
		フロー レコード コンフィギュレーション モードを開始します。

ステップ 4	**match datalink** {**dot1q** |**ethertype**	**mac**	**vlan**} 例： `Device(config-flow-record)# match datalink ethertype`	レイヤ 2 属性をキーとして指定します。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Device(config-flow-record)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show flow record** [*name*] 例： `Device# show flow record`	（任意）インターフェイスの NetFlow 情報を表示します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

Flexible NetFlow の監視

次の表にあるコマンドを使用して、Flexible NetFlow をモニタリングできます。

表 *4 : Flexible NetFlow* のモニタリング コマンド

コマンド	目的
show flow exporter [**broker** | **export-ids** | **name** | *name* | **statistics** | **templates**]	NetFlow のフロー エクスポータ情報と統計情報を表示します。
show flow exporter [**name** *exporter-name*]	NetFlow のフロー エクスポータ情報と統計情報を表示します。
show flow interface	NetFlowインターフェイスに関する情報を表示します。
show flow monitor [**name** *exporter-name*]	NetFlow のフロー モニタ情報と統計情報を表示します。
show flow monitor statistics	フロー モニタの統計情報を表示します。
show flow monitor cache format {**table** | **record** | **csv**}	指定された形式でフロー モニタのキャッシュの内容を表示します。
show flow record [**name** *record-name*]	NetFlowのフロー レコード情報を表示します。

コマンド	目的
show sampler [**broker** | **name** | *name*]	NetFlow サンプラーに関する情報を表示します。

Flexible NetFlow の設定例

例：フローの設定

フローを作成し、そのフローをインターフェイスに適用する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

Device(config)# flow export export1
Device(config-flow-exporter)# destination 10.0.101.254
Device(config-flow-exporter)# transport udp 2055
Device(config-flow-exporter)# exit
Device(config)# flow record record1
Device(config-flow-record)# match ipv4 source address
Device(config-flow-record)# match ipv4 destination address
Device(config-flow-record)# match ipv4 protocol
Device(config-flow-record)# match transport source-port
Device(config-flow-record)# match transport destination-port

Device(config-flow-record)# collect counter byte long
Device(config-flow-record)# collect counter packet long
Device(config-flow-record)# collect timestamp absolute first
Device(config-flow-record)# collect timestamp absolute last
Device(config-flow-record)# exit
Device(config)# flow monitor monitor1
Device(config-flow-monitor)# record record1
Device(config-flow-monitor)# exporter export1
Device(config-flow-monitor)# exit
Device(config)# interface tenGigabitEthernet 1/0/1
Device(config-if)# ip flow monitor monitor1 input
Device(config-if)# end
```

例：IPv4 入力トラフィックのモニタリング

次の例は、IPv4 入力トラフィックをモニタする方法を示しています（int g1/0/11 は、int g1/0/36 および int g3/0/11 にトラフィックを送信します）。

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# flow record  fr-1
Device(config-flow-record)# match ipv4 source address
Device(config-flow-record)# match ipv4 destination address
Device(config-flow-record)# match interface input
```

```
Device(config-flow-record)# collect counter bytes long
Device(config-flow-record)# collect counter packets long
Device(config-flow-record)# collect timestamp absolute first
Device(config-flow-record)# collect timestamp absolute last
Device(config-flow-record)# collect counter bytes layer2 long
Device(config-flow-record)# exit

Device(config)# flow exporter fe-ipfix6
Device(config-flow-exporter)# destination 2001:0:0:24::10
Device(config-flow-exporter)# source Vlan106
Device(config-flow-exporter)# transport udp 4739
Device(config-flow-exporter)# export-protocol ipfix
Device(config-flow-exporter)# template data timeout 240
Device(config-flow-exporter)# exit

Device(config)# flow exporter fe-ipfix
Device(config-flow-exporter)# description IPFIX format collector 100.0.0.80
Device(config-flow-exporter)# destination 100.0.0.80
Device(config-flow-exporter)# dscp 30
Device(config-flow-exporter)# ttl 210
Device(config-flow-exporter)# transport udp 4739
Device(config-flow-exporter)# export-protocol ipfix
Device(config-flow-exporter)# template data timeout 240
Device(config-flow-exporter)# exit

Device(config)# flow exporter fe-1
Device(config-flow-exporter)# destination 10.5.120.16
Device(config-flow-exporter)# source Vlan105
Device(config-flow-exporter)# dscp 32
Device(config-flow-exporter)# ttl 200
Device(config-flow-exporter)# transport udp 2055

Device(config-flow-exporter)# template data timeout 240
Device(config-flow-exporter)# exit

Device(config)# flow monitor fm-1
Device(config-flow-monitor)# exporter fe-ipfix6
Device(config-flow-monitor)# exporter fe-ipfix
Device(config-flow-monitor)# exporter fe-1
Device(config-flow-monitor)# cache timeout inactive 60
Device(config-flow-monitor)#  cache timeout active 180
Device(config-flow-monitor)# record fr-1
Device(config-flow-monitor)# end

Device# show running-config interface g1/0/11
Device# show running-config interface g1/0/36
Device# show running-config interface g3/0/11
Device# show flow monitor fm-1 cache format table
```

例：IPv4 出力トラフィックのモニタリング

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# flow record  fr-1 out
Device(config-flow-record)# match ipv4 source address
Device(config-flow-record)# match ipv4 destination address
Device(config-flow-record)# match interface output
Device(config-flow-record)# collect counter bytes long
```

```
Device(config-flow-record)# collect counter packets long
Device(config-flow-record)# collect timestamp absolute first
Device(config-flow-record)# collect timestamp absolute last
Device(config-flow-record)# exit

Device(config)# flow exporter fe-1
Device(config-flow-exporter)# destination 10.5.120.16
Device(config-flow-exporter)# source Vlan105
Device(config-flow-exporter)# dscp 32
Device(config-flow-exporter)# ttl 200
Device(config-flow-exporter)# transport udp 2055
Device(config-flow-exporter)# template data timeout 240
Device(config-flow-exporter)# exit

Device(config)# flow exporter fe-ipfix6
Device(config-flow-exporter)# destination 2001:0:0:24::10
Device(config-flow-exporter)# source Vlan106
Device(config-flow-exporter)# transport udp 4739
Device(config-flow-exporter)# export-protocol ipfix
Device(config-flow-exporter)# template data timeout 240
Device(config-flow-exporter)# exit

Device(config)# flow exporter fe-ipfix
Device(config-flow-exporter)# description IPFIX format collector 100.0.0.80
Device(config-flow-exporter)# destination 100.0.0.80
Device(config-flow-exporter)# dscp 30
Device(config-flow-exporter)# ttl 210
Device(config-flow-exporter)# transport udp 4739
Device(config-flow-exporter)# export-protocol ipfix
Device(config-flow-exporter)# template data timeout 240
Device(config-flow-exporter)# exit

Device(config)# flow monitor fm-1-output
Device(config-flow-monitor)# exporter fe-1
Device(config-flow-monitor)# exporter fe-ipfix6
Device(config-flow-monitor)# exporter fe-ipfix
Device(config-flow-monitor)# cache timeout inactive 50
Device(config-flow-monitor)#  cache timeout active 120
Device(config-flow-monitor)# record fr-1-out
Device(config-flow-monitor)# end

Device# show flow monitor fm-1-output cache format table
```

Flexible NetFlow の機能情報

リリース	変更内容
Cisco IOS XE Everest 16.6.1	この機能が導入されました。
Cisco IOS XE Gibraltar 16.12.1	IPv6 トラフィックについて、FNF の SGT フィールドと DGT フィールドのサポートが導入されました。

リリース	変更内容
Cisco IOS XE Amsterdam 17.1.1	MPLS（IP レベル）での入力および出力 Flexible Netflow のサポートが導入されました。
Cisco IOS XE Amsterdam 17.2.1	Flexible Netflow で VPN ID を設定するためのサポートが導入されました。